UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BYTEMARK, INC.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**CIVIL ACTION NO. 1:17-cv-01803**
	§	**(PGG)**
XEROX CORP., ACS TRANSPORT SOLUTIONS, INC., XEROX TRANSPORT SOLUTIONS, INC., CONDUENT INC., and NEW JERSEY TRANSIT CORP.,	§	**ECF CASE**
	§	
	§	
	§	
	§	
	§	
Defendants.	§	
	§	
	§	
	§	
	§	

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION TO COMPEL AND MOTION FOR PROTECTIVE ORDER

Table of Contents

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

Pursuant to Federal Rule of Civil Procedure 37, Local Civil Rule 6.1 for the Southern District of New York, and this Court's Order (Dkt. No. 110), Defendants Xerox Corp., ACS Transport Solutions, Inc., Xerox Transport Solutions, Inc., Conduent, Inc., and New Jersey Transit Corp. (collectively, "Defendants") file this Memorandum of Law in Support of Its Motion to Compel and Motion for Protective Order ("Motion") against Plaintiff Bytemark, Inc. ("Bytemark").

Specifically, Defendants request an order compelling Bytemark to identify the allegedly misappropriated trade secrets that form Bytemark's good-faith basis for filing this lawsuit. Defendants also request that the Court enter a Protective Order preventing Bytemark from conducting a fishing expedition into Defendants' proprietary source code and other confidential engineering documents (collectively, "confidential information") prior to Bytemark identifying its allegedly misappropriated trade secrets.

I. **Introduction**

The crux of this discovery dispute is whether Bytemark should be given access to all of Defendants' confidential information before identifying its alleged trade secrets. It should not. Courts in this district and others consistently require plaintiffs, like Bytemark, to identify their trade secrets with reasonable particularity prior to discovery. This rule makes sense. Bytemark should not be allowed to obtain full disclosure of Defendants' confidential information and then tailor its alleged trade secrets accordingly. A trade secret disclosure from Bytemark also narrows the case and ensures efficient adjudication for all parties. For these reasons, Defendants respectfully request that the Court order Bytemark to identify its allegedly misappropriated trade secrets with reasonable particularity before granting Bytemark access to Defendants' confidential information.

II. Factual Background

On March 10, 2017, Plaintiff Bytemark filed its Original Complaint against Defendants for alleged trade secret misappropriation, among other things. In its Complaint, Bytemark vaguely and broadly identified its alleged trade secrets as "proprietary mobile ticket development technology and know-how, design and implementation of mobile ticketing technology applications . . . , back-end application and system management, maintenance and service, user data and account management and associated security features, and aspects of Bytemark's pricing, sales initiatives and profit generation paradigm." Ex. A (Bytemark's Original Complaint) at ¶ 66; *see also* ¶¶ 26, 76.

On October 23, 2018, Defendants requested via interrogatory and Request for Production that Bytemark specify with particularity its alleged trade secrets. Ex. B (Defendants First Set of Interrogatories) at Interrogatory 1; Ex. C (Defendants First Set of Requests for Production) at RFP 1-6. Bytemark, citing Local Rule 33.3, refused to identify it alleged trade secrets. Ex. D (Bytemark's Response to Defendants First Set of Interrogatories) at Interrogatory 1.

In March of 2019, after multiple conferences, Defendants proposed a compromise where it would inspect Bytemark's universe of trade secrets so that they could begin to understand Bytemark's allegations and the information that may be relevant to this case. With that understanding in hand, Defendants could then search for, collect, and produce Defendant's confidential information. Even though Bytemark would likely produce a large amount of irrelevant information (while knowing full well the trade secrets it believes Defendants misappropriated), Defendants proposed this compromise to avoid burdening the Court. Bytemark rejected Defendants' proposal. Ex. E.

Bytemark then sat idle on this issue for more than a year. In June 2020, Bytemark resurrected trade secret disclosure discussions, once more demanding the right to troll through all of Defendant's confidential information without first limiting the case to information relevant to Bytemark's allegations. Hoping to reach a resolution, Defendants again offered a framework to avoid motion practice. First, Bytemark would make the universe of its alleged trade secret material available for inspection. Second, Defendants' would make its confidential information available for inspection. And third, Bytemark would identify its trade secrets with particularity. Ex. F at 9-11. Due to the COVID-19 pandemic, Defendants prepared a detailed stipulation that established remote review procedures. *Id*. at 5-8 Bytemark refused Defendants' proposal. *Id*. at 2-3. In the spirit of compromise, Defendants then proposed alternative in-person review procedures that would ensure the health and safety of all parties involved. *Id*. at 2. Bytemark again declined. Simply put, Bytemark was unwilling to agree to any compromise that required it to identify its alleged trade secrets with particularity. Bytemark's final word was to refuse any agreement and institute motion practice. *Id*. at 1.

III. Argument

A. This jurisdiction and others require identification of trade secrets with reasonable particularity prior to discovery.

Bytemark's position that it need not identify its alleged trade secrets until the close of fact discovery, long after it reviews Defendants' confidential information, is contrary to the holdings of numerous courts that have examined this issue. For the same reason that a lost-and-found requires a description before releasing a lost item, courts require that a plaintiff must identify its trade secrets early in discovery. Otherwise, a plaintiff could make broad allegations of misappropriation, obtain full access to a defendant's confidential information, and then tailor its trade secrets accordingly.

Citing fairness rationales, New York courts require a trade secret plaintiff like Bytemark to disclose its trade secrets before discovering a defendant's confidential information. For example, in *MSCI Inc. v. Jacob*, the New York state court noted the inherent unfairness if a plaintiff were allowed "discover [defendants'] trade secrets prior to revealing their own." 36 Misc. 3d 211, 214-15, 945 N.Y.S.2d 863, 866 (Sup. Ct. 2012). Since a plaintiff brings an action for trade secret misappropriation, the plaintiff "bear[s] the burden of proving [its] allegation." *Id.* at 865. If, as Bytemark proposes in this case, "defendants remain in the dark as to the explicit [information] that plaintiffs deem to be trade secrets misappropriated by defendants, plaintiffs, once privy to [defendants'] source codes, could tailor their theory of misappropriation to [defendants'] work." *Id.* at 866. To prevent this unfairness, the court precluded the plaintiffs "from seeking further discovery from defendants until they identify, with reasonable particularity, which of the component parts or sequencing of their source code are not (1) publicly available information, (2) commonly-used algorithms, or (3) third-party licensing." *Id*; *see also Power Conversion, Inc. v. Saft America, Inc.*, No. 83 Civ. 9185, 1985 WL 1016, at *2

(S.D.N.Y. May 1, 1985) (sustaining objection to magistrate judge's ruling and requiring plaintiff to disclose its trade secrets in camera prior to discovery).

New York is not the only jurisdiction to recognize the high risk of unfairness if a plaintiff like Bytemark can conceal its trade secrets until late in discovery. In *Powerweb Energy, Inc. v. Hubbell Lighting, Inc.*, a Connecticut court granted defendant's motion for protective order and ordered plaintiff "to provide defendants with a description that defines with reasonable specificity the alleged trade secrets which form the basis of its misappropriation claim." *Powerweb Energy, Inc. v. Hubbell Lighting, Inc.*, Civ. No. 3:12CV220 (WWE), 2012 WL 3113162 at *2 (D. Conn. 2012). "Of paramount concern to the [c]ourt [was] fairness and efficiency." *Id*. The risk that plaintiff would incur an unfair advantage by crafting its broad trade secret allegations to match defendant's confidential material was too great.

Indeed, multiple other jurisdictions have established disclosure requirements to prevent unfair tactics by trade secret plaintiffs. Delaware's common law requires a trade secret plaintiff to "identify with reasonable particularity the matter which it claims constitutes a trade secret" before discovering defendant's confidential information. *Engelhard Corp. v. Savin Corp.*, 505 A.2d 30, 33 (Del. Ch. 1986). Illinois and Florida likewise require trade secret identification before discovery. *See AutoMed Techs., Inc. v. Eller*, 160 F. Supp. 2d 915, 926 (N.D. Ill. 2001) (citing Delaware case law, prohibiting discovery until the plaintiff "particularize[d] which of its secrets were allegedly misappropriated"); *Del Monte Fresh Produce Co. v. Dole Food Co. Inc.*, 148 F. Supp. 2d 1322, 1326 (S.D. Fla. 2001) (requiring plaintiff to "list and reasonably describe the trade secrets it seeks to protect").

The inequitable consequences of a plaintiff identifying its trade secrets after reviewing a defendant's confidential information has even prompted California to statutorily mandate trade secret disclosures. California's Civil Procedure Code § 2019.210 states that "before commencing discovery relating to the trade secret, the party alleging the misappropriation shall identify the trade secret with reasonable particularity subject to any [protective] orders." *See also Computer Economics, Inc. v. Gartner Group, Inc.*, 50 F. Supp.2d at 983-984 (S.D. Cal. 1999) (applying California's trade secret requirement in a federal case). The same fairness concerns that motivated California to codify trade secret disclosure requirements likewise compel Bytemark to identify its trade secrets in this case.

In addition to fairness concerns, Bytemark should be required to identify its trade secrets because it streamlines litigation. Federal courts have found that pre-discovery identification of trade secrets serves several beneficial purposes:

> "First, [it] promotes well-investigated claims and dissuades the filing of meritless trade secret complaints. Second, it prevents plaintiffs from using the discovery process as a means to obtain defendant's trade secrets. Third, the rule assists the court in framing the appropriate scope of discovery and in determining whether plaintiff's discovery requests fall within that scope. Fourth, it enables defendants to form complete and well-reasoned defenses, ensuring that they need not wait until the eve of trial to effectively defend against charges of trade secret misappropriation."

Loop AI Labs, Inc. v. Gatti, 195 F.Supp.3d 1107 (N.D. Cal. 2016). In this case, a trade secret disclosure from Bytemark would enable the parties and the Court to narrow the issues and provide meaningful, targeted, and relevant discovery. Absent such a disclosure, the uncertainty in Bytemark's claims will lead to unnecessary disputes, inefficient motions practice, and burdensome discovery.

In sum, the overwhelming majority of courts, and the compelling fairness and efficiency rationales, support Defendants' request that Bytemark be compelled to identify its trade secrets with reasonable particularity. This can be done through a specific trade secret disclosure or a response to Interrogatory No. 1. Until Bytemark identifies its alleged trade secrets with reasonable particularity, Defendants respectfully request a Protective Order postponing their production of confidential source code and related documentation until after Bytemark identifies its alleged trade secrets with reasonable particularity.

B. Bytemark has not identified its trade secrets with sufficient reasonable particularity.

In its letter brief to the Court, Bytemark erroneously claims that it has identified its trade secrets with sufficient particularity. In support of its claim, Bytemark cites *Uni-Sys., LLC v. U.S. Tennis Ass'n* for the proposition that only a very general showing of trade secrets may be necessary early in the case. No. 17CV147KAMCLP, 2017 WL 4081904, at *4 (E.D.N.Y. Sept. 13, 2017). But this is not the full opinion. Just a few lines prior to Bytemark's pincite, the court makes clear that "federal courts regularly require trade secrets plaintiffs to identify alleged trade secrets with 'reasonable particularity.'" *Id.* And just a few lines after Bytemark's pincite, the Court unambiguously states that "[i]t is clear, however, that generic descriptions of categories are insufficient to provide defendants with information sufficient to satisfy the 'reasonable particularity' standard." *Id.* The very case Bytemark cites shows New York courts require more than generic descriptions of broad trade secret categories.

Nevertheless, despite being nearly three years into this litigation, Bytemark has provided only generic descriptions of it alleged trade secrets. In fact, the only description of Bytemark's alleged trade secrets appears in three nearly-identical paragraphs in its Complaint. Ex. A (Bytemark's Original Complaint) at ¶¶ 26, 66, 76. These paragraphs merely state that

Bytemark's trade secrets encompass generic categories such as "back-end application and system management," and are insufficient to meet its obligations. This stands in stark contrast to the plaintiff in *Uni-Sys* who provided "36 pages describing their alleged trade secret." *Uni-Sys., LLC*, 2017 WL 4081904 at *4.

Thus, under the very cases it cites, Bytemark has failed to identify its trade secrets with sufficient particularity. Consistent with this Court's precedent, and the precedent of similarly-situated jurisdictions, Defendants respectfully request that a Protective Order be entered preventing Bytemark from discovering Defendants' confidential information until Bytemark provides a sufficiently detailed trade secret disclosure.

C. Local Rule 33.3 does not excuse Bytemark from its obligation to identify its alleged trade secrets with reasonable particularity.

Bytemark's refusal to identify its trade secrets pursuant to Interrogatory No. 1 is based on a misreading of Local Rule 33.3(a) and (c). While this Local Rule limits the use of interrogatories in certain scenarios, none of them shield Bytemark here. Local Rule 33.3(a) applies "at the commencement of discovery," not three years after a case is filed and more than eighteen months into discovery. More importantly, associated Local Rule 33.3(b) allows for interrogatories other than those permitted by 33.3(a) "if they are a more practical method of obtaining the information sought than a request for production or a deposition." Defendants' Interrogatory No. 1 meets this criterion. It is Bytemark's burden to identify its trade secrets with reasonable particularity, and neither a deposition nor a document production are preferred avenues for that identification. *See, e.g., Big Vision Private v. E.I. DuPont De Nemours & Co.*, 1 F.Supp.3d 224, 263 (S.D.N.Y. 2014) ("[Plaintiff] impermissibly shifts its burden onto [defendant] (and the Court) to sift through 70 pages of abstruse laboratory papers to ascertain [plaintiff's] trade secret.").

D. Defendants have established good cause for a protective order.

Defendants recognize that they must establish good cause for entry of their requested protective order. Fed. R. Civ. P. 26(c). Good cause exists here. Under Rule 26(c), the trial court has "broad discretion ... to decide when a protective order is appropriate and what degree of protection is required." *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 36, 104 S. Ct. 2199, 2209, 81 L. Ed. 2d 17 (1984). Good cause is established by "demonstrating a particular need for protection." *Cipollone v. Liggett Grp., Inc.*, 785 F.2d 1108, 1121 (3d Cir. 1986); *see also In re Terrorist Attacks on Sept. 11, 2001*, 454 F.Supp.2d 220, 222 (S.D.N.Y.2006) (Casey, D.J.) ("Ordinarily, good cause [for a protective order] exists when a party shows that disclosure will result in a clearly defined, specific and serious injury.") (internal quotations and citations omitted); *Koster v. Chase Manhattan Bank*, 93 F.R.D. 471, 479 (S.D.N.Y.1982).

As outlined above, Defendants will be harmed if Bytemark is permitted to view Defendants' confidential information without first providing a trade secret disclosure. Absent a protective order, Bytemark will tailor its alleged trade secrets to what it discovers in Defendants' confidential information. In addition, Defendants will be forced to produce a vast amount of irrelevant, yet highly-sensitive, confidential information to respond to Bytemark's discovery. This is extremely burdensome to Defendants. A trade secret disclosure from Bytemark will narrow the scope of discovery, minimize the burden and prejudice to Defendants, and improve efficiency for the Court and the parties. *See Buzzeo v. Bd. of Educ., Hempstead*, 178 F.R.D. 390, 393 (E.D.N.Y. 1998) *(*granting motion for protective order after performing "an analysis of cost, convenience and litigation efficiency"*).*

A protective order also balances Bytemark's interest in full disclosure with Defendants' interest in preventing harm and unfairness. Bytemark is aware of all the information over which it claims trade secret protection. Bytemark is also aware of all the information it disclosed to

Defendants. Bytemark is thus in a unique position to provide a disclosure identifying all of its alleged trade secrets with minimal effort. Upon such a disclosure, Defendants will discharge their obligation to produce all relevant confidential information to Bytemark.

IV. Conclusion

For the reasons explained above, Defendants request that the Court order Bytemark to identify its trade secrets with reasonable particularity either via a trade secret disclosure or a response to Interrogatory No. 1. Until Bytemark makes this identification, Defendants also seek a Protective Order preventing Bytemark from pursuing the entirety of Defendants' confidential information in an attempt to tailor its trade secrets to fit what it finds there.

Dated: December 28, 2020

Respectfully submitted,

/s/ Ashley N. Moore
Ashley N. Moore (admitted *pro hac vice*)
David Sochia (admitted *pro hac vice*)
Douglas A. Cawley (admitted *pro hac vice*)
Marcus L. Rabinowitz (admitted *pro hac vice*)

McKool Smith, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Tel: (214) 978-4000
Fax: (214) 978-4044
amoore@mckoolsmith.com
dsochia@mckoolsmith.com
dcawley@mckoolsmith.com
mrabinowitz@mckoolsmith.com

David R. Dehoney (4616595)
McKool Smith, P.C.
One Bryant Park, 47th Floor
New York, New York 10036
Tel: (212) 402-9424
Fax: (212) 402-9444
ddehoney@mckoolsmith.com

Attorneys for Defendants